

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

01/08/2013

SUBJECT:

Vulnerabilities in .NET Framework Could Allow Remote Code Execution (MS13-004)

OVERVIEW:

Four vulnerabilities have been discovered in the Microsoft .NET Framework, some of which could allow an attacker to take complete control of an affected system. Microsoft .NET is a software framework for applications designed to run under Microsoft Windows. These vulnerabilities can be exploited if a user visits or is redirected to a malicious web page or runs a specially crafted Microsoft.NET application.

Successful exploitation of these vulnerabilities could allow an attacker to obtain complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft .NET Framework 1.0
- Microsoft .NET Framework 1.1
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Four vulnerabilities have been discovered in the Microsoft .NET Framework, details of which are described below:

System Drawing Information Disclosure Vulnerability (CVE-2013-0001) – An information disclosure vulnerability exists in the way that the .NET Framework initializes the contents of a memory array. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code Access Security (CAS) restrictions.

WinForms Buffer Overflow Vulnerability (CVE-2013-0002) - An elevation of privilege vulnerability exists in the way that the .NET Framework validates the number of objects in memory before copying to an array. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass CAS restrictions. By default, Internet Explorer 9 and Internet Explorer 10 prevent XAML, which is used by XBAPs, from running in the Internet Zone. Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 are configured to prompt the user before running XAML, which is used by XBAPs in the Internet Zone.

S.DS.P Buffer Overflow Vulnerability (CVE-2013-0003) - An elevation of privilege vulnerability exists in the way that the .NET Framework validates the size of objects in memory before copying to an array. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass CAS restrictions.

Double Construction Vulnerability (CVE-2013-0004) - An elevation of privilege vulnerability exists in the way that the .NET Framework validates the permissions of an object in memory. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP content using Internet Explorer. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass CAS restrictions. By default, Internet Explorer 9 and Internet Explorer 10 prevent XAML, which is used by XBAPs, from running in the Internet Zone. Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 are configured to prompt the user before running XAML, which is used by XBAPs in the Internet Zone.

Successful exploitation of these vulnerabilities could result in the execution of the attacker-supplied code and allow the attacker to obtain complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Unless there is a business need to do otherwise, consider disabling XAML browser applications (XBAP) in Internet Explorer 6, 7, 8. By default, Internet Explorer 9 and Internet Explorer 10 prevent XAML, which is used by XBAPs

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms13-004>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0001>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0002>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0003>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0004>

SecurityFocus:

<http://www.securityfocus.com/bid/57113>

<http://www.securityfocus.com/bid/57114>

<http://www.securityfocus.com/bid/57124>

<http://www.securityfocus.com/bid/57126>